Army Regulation 381–11

Military Intelligence

Threat Support to U.S. Army Force, Combat, and Materiel Development

Headquarters
Department of the Army
Washington, DC
12 March 1986

SUMMARY of CHANGE

AR 381-11
Threat Support to U.S. Army Force,
Combat, and Materiel Development

This revision—

- o Provides guidance on the development of threat support programs and use of approved intelligence products (para 2-1).

- o Introduces the responsibilities of the threat integration staff officers and the functions of threat coordinating groups (paras 2-4 and 2-5).

- o Changes the responsibilities for the preparation, review, and approval of system specific threat assessments (para 2-6).

Headquarters
Department of the Army
Washington, DC
12 March 1986

*Army Regulation 381–11

Effective 14 April 1986

Military Intelligence

Threat Support to U.S. Army Force, Combat, and Materiel Development

This UPDATE printing publishes a revision which is effective 14 April 1986. Because the structure of the entire revised text has been reorganized, no attempt has been made to highlight changes from the earlier regulation dated 15 August 1981.

By Order of the Secretary of the Army:

JOHN A. WICKHAM, JR.
General, United States Army
Chief of Staff

Official:

R. L. DILWORTH
Brigadier General, United States Army
The Adjutant General

Summary. This regulation governs threat support to the U.S. Army force, combat, and materiel development process. It provides guidance on the development of threat support programs, use of approved intelligence products, responsibilities of the Office of the Assistant Chief of Staff for Intelligence threat integration staff officers, and the functions of threat coordinating groups.

Applicability. This regulation applies to elements of the Active Army engaged in force, combat, and materiel development activities. It does not apply to the Army National Guard (ARNG) or the U.S. Army Reserve (USAR).

Impact on New Manning System. This regulation does not contain information that affects the New Manning System.

Internal control systems. This regulation is subject to the requirements of AR 11–2. It contains internal control provisions but does not contain checklists for conducting internal control reviews. These checklists are being developed and will be published at a later date.

Supplementation. Supplementation of this regulation and establishment of forms other than DA forms are prohibited, unless prior approval is obtained from HQDA (DAMI–FIT), WASH DC 20310–1086.

Interim changes. Interim changes to this regulation are not official unless they are authenticated by The Adjutant General. Users will destroy interim changes on their expiration date unless sooner superseded or rescinded.

Suggested Improvements. The proponent agency of this regulation is the Office of the Assistant Chief of Staff for Intelligence. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMI–FIT), WASH DC 20310–1086.

Distribution. Distribution of this issue has been made in accordance with DA Form 12–9A requirements for 381 series publications. The number of copies distributed to a given subscriber is the number of copies requested in Block 339 of the subscriber's DA Form 12–9A. AR 381–11 distribution is D for Active Army, none for ARNG, and none for USAR.

Contents (Listed by paragraph number)

*This regulation supersedes AR 381-11, 15 August 1981.

RESERVED

Chapter 1 General

1–1. Purpose

This regulation prescribes policies, responsibilities, and procedures for providing threat support to the Army's force, combat, and materiel development process. It provides guidance on the purpose, content, and focus of threat assessments used in support of force, combat, and materiel development activities. This regulation is intended to ensure that threat support helps guide the Army's force modernization effort.

1–2. References

Required and related references are listed in appendix A.

1–3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1–4. Responsibilities

a. The Assistant Chief of Staff for Intelligence will—

(1) Establish threat support policy.

(2) Approve threat documentation designated for Army Systems Acquisition Review Council (ASARC) or Defense Systems Acquisition Review Council (DSARC) decision (table 2–1) and studies in support of the Headquarters, Department of the Army (HQDA) decision process.

(3) Review and monitor the threat support process to ensure consistent application of threat in support of major and DAP systems and HQDA-directed studies.

(4) Review and validate critical intelligence parameters (CIPs).

(5) Provide for representation to special task forces (STF), special study groups (SSGs), and study advisory groups (SAGs) for studies requiring threat consideration.

(6) Serve as a member of the Army System Acquisition Review Council.

(7) Establish and chair HQDA threat coordinating groups (TCGs) for major and Designated Acquisition Program (DAP) systems and determine the appropriateness for establishing HQDA TCGs for other programs or studies.

(8) Review and approve all aspects of threat portrayed during the development of U.S. Army Training and Doctrine Command (TRADOC) standard scenarios.

b. The Deputy Chief of Staff for Operations and Plans (DCSOPS) will—

(1) Coordinate with the Office of the Assistant Chief of Staff for Intelligence (OACSI) on requirements for threat support.

(2) Ensure that the following materiel requirements documents which are prepared at various points in the life cycle of a major or DAP system contain, reference, or reflect, HQDA-approved threat assessments.

(a) Justification for Major System New Start (JMSNS).

(b) Operational and Organizational (O&O) Plan.

(c) Letter of Agreement (LOA).

(d) Required operational capability (ROC).

(e) Joint Service Operational Requirement (JSOR).

(3) Coordinate with OACSI on appropriate threat guidance and policies for cost and operational effectiveness analysis (COEA).

(4) Coordinate with OACSI for threat representation on each special task force.

(5) Coordinate with OACSI for the integration of Army-approved threat in user test programs, including operational tests (OTs), force development testing and experimentation (FDTE), and joint operational testing.

(6) Participate in HQDA level TCGs for the coordination of threat support to the force, combat, and materiel development process.

(7) Coordinate with OACSI for the integration of threat support guidance in all study directives, and analysis and guidance documents.

c. The Deputy Chief of Staff for Research, Development, and Acquisition (DCSRDA) will—

(1) Coordinate with OACSI on research, development, and acquisition requirements for threat support.

(2) Ensure that the following documents that are prepared to support milestone decision reviews for major and DAP systems contain or reference HQDA-approved threat assessments:

(a) System concept paper (SCP).

(b) Decision coordinating paper (DCP).

(c) Integrated program summary (IPS).

(3) Provide for the integration of threat support in all study directives and guidance documents from earliest concept stages.

(4) Coordinate with OACSI in developing the Long-range Research, Development, and Acquisition Plan (LRRDAP) to ensure that intelligence assets are programmed to support long-range planning initiatives, and that the plan reflects consideration of the threat.

(5) Coordinate with OACSI to ensure that approved threat statements and appropriate threat guidance and policies are present in the management of Product Improvement Proposals (PIPs).

(6) Participate in HQDA-level TCGs for the coordination of threat support to the force, combat, and materiel development process.

(7) Ensure that approved intelligence data and threat assessments are integrated into developmental testing.

d. The Commanding General, U.S. Army Training and Doctrine Command will—

(1) In coordination with the U.S. Army Materiel Command (AMC), prepare, review, and forward to OACSI for DA approval all threat statements developed for each JMSNS, O&O Plan, LOA, ROC, and JSOR for major and DAP systems.

(2) In coordination with AMC, prepare, review, and approve all threat statements developed for each O&O Plan, LOA, and JSOR for Department of the Army (DA) in-process review (DAIPR) and in-process review (IPR) level systems. Provide information copies to OACSI and U.S. Army Intelligence Agency (USAIA).

(3) Prepare, in coordination with AMC and the appropriate HQDA TCG, and forward to OACSI for approval all System Threat Assessment Reports (STARs) for major and DAP systems.

(4) Develop, in coordination with AMC and OACSI, command threat support requirements to include the identification of CIPs for specific programs and studies.

(5) Develop, produce, and coordinate the threat portion of TRADOC standard scenarios and forward to OACSI for approval.

(6) Provide for threat representation on each special study group and identify threat support requirements to OACSI.

(7) Participate in DA-level TCGs.

(8) In coordination with AMC, establish appropriate TCGs to provide threat support to DAIPR and IPR level systems.

(9) Coordinate with OACSI to ensure the provision of appropriate threat support to each mission area analysis (MAA).

(10) Prepare, in coordination with AMC and the appropriate HQDA TCG, a threat support plan for each major and DAP system.

(11) Prepare, in coordination with AMC, a threat support plan and the STAR for DAIPR and IPR systems.

(12) Ensure the integration of approved threat in user testing programs to include the preparation of test threat support packages in response to stated tester requirements.

e. The Commanding General, U.S. Army Materiel Command will—

(1) In coordination with TRADOC, prepare, review, and forward to OACSI for HQDA approval all threat statements developed for each SCP, DCP, and IPS for major and DAP systems.

(2) In coordination with TRADOC, prepare, review, and approve all threat statements developed for each SCP, DCP, and IPS for DAIPR and IPR level system and provide information copies to OACSI and USAIA.

(3) Develop, in coordination with TRADOC and OACSI, command threat support requirements to include identification of CIPs for specific programs and studies.

(4) Coordinate with TRADOC the preparation of STARs for major, DAP, DAIPR, and IPR systems.

(5) Ensure the integration of approved threat in developmental test programs.

(6) Participate in DA level TCGs.

(7) In coordination with TRADOC, establish appropriate TCGs to provide threat support for DAIPR and IPR level systems.

(8) Participate with TRADOC in the preparation of threat support plans for major, DAP, DAIPR, and IPR systems.

f. The Commander, U.S. Army Intelligence Agency will—

(1) Produce current and projected general and scientific and technical intelligence (S&TI).

(2) Produce intelligence documents and S&TI quantitative data in automated format to support specific force, combat, and materiel development programs.

(3) Participate in TCGs to support the force, combat, and materiel development process.

(4) Assist in the development and the review of the application of threat in selected combat and materiel developers' acquisition programs, studies, developmental and operational tests, and combat simulations and wargames. This will include the Army Development and Acquisition of Threat Simulators (ADATS) Program.

(5) Provide representatives to work groups and TCGs formed to support HQDA and major Army command (MACOM) directed studies and analyses.

(6) Develop and maintain threat data base as directed by OACSI.

(7) Develop threat analysis and forecasting methodologies.

(8) Assist developers in the development of intelligence production requirements and the definition of critical intelligence parameters.

g. The Director, Armed Forces Medical Intelligence Center will—

(1) Produce current and projected general medical and scientific and technical intelligence.

(2) Produce intelligence documents to support specific force, combat, and materiel development programs.

(3) Participate in DA-level TCGs for the coordination of threat support to the combat and materiel development process.

h. The Commanding General, U.S. Army Operational Test and Evaluation Agency (OTEA) will—

(1) Coordinate test planning with the appropriate threat approval authority (table 2–1) to ensure that an appropriate battlefield environment is portrayed.

(2) Participate in TCGs to ensure that threat requirements to support testing are identified as early as possible after program initiation.

i. The Director, U.S. Army Concepts Analysis Agency (CAA) will—

(1) Develop, in coordination with OACSI and DCSOPS, threat support requirements for theater level wargaming.

(2) Participate in DA level TCGs involving force development issues.

(3) Coordinate with OACSI to ensure the provision of appropriate threat support to HQDA-sponsored force development studies.

j. Other developers and testers not specifically identified in this regulation will assume the same basic responsibilities and relationships with the threat support agencies as TRADOC and AMC.

1–5. Policies

DOD Instruction 5000.2 contains guidance on threat support to materiel acquisition. It states that the effectiveness of a proposed weapon system in its intended threat environment must be a fundamental concern of the acquisition effort and must be considered by program managers from the outset. DIA Regulation 55–3 contains detailed guidance on threat support to major system acquisitions. Policies for threat support to force, combat, and materiel development as they pertain to the Army are as follows:

a. Consideration of threat is a command responsibility. Commanders at all levels will ensure that approved threat is applied and integrated into force, combat, and materiel development programs.

b. Threat will be derived from Army- and DIA-approved scientific and technical intelligence (characteristics, capabilities, and limitations of foreign equipment) and general intelligence (organization, doctrine, and tactics of threat forces). The reformatting of approved intelligence data to meet threat requirements is the responsibility of the proponent threat support office.

c. The U.S. Army Intelligence Agency will produce both general and scientific and technical intelligence in response to approved requirements.

d. The combat and materiel development commands will prepare required threat documentation, to include threat assessments, to support the specific combat and materiel development activities for which those commands are responsible.

e. Intelligence producers will provide threat support in response to developers' guidance and defined requirements for all force, combat, and materiel development-related activities including Planning, Programing, and Budgeting System (PPBS), mission area analysis, cost and operational effectiveness analyses, development tests, and operational tests.

f. The senior intelligence officer (SIO) of each command and activity involved in the force, combat, and materiel development process will review and approve threat assessments written in support of command missions before forwarding them to the next higher level of command.

Chapter 2 Threat Support

Section I Threat Support Programs

2–1. General

a. The purpose of threat support programs is to ensure that force, concepts, doctrine, training, organization, and materiel systems which most effectively and efficiently respond to the evolving threat environment are developed. Threat support must be timely, consistent, and continuous to achieve this purpose.

(1) Timeliness ensures that threat considerations are provided to combat and materiel developers at critical points in the combat and materiel development cycle in order to properly influence the requirement for and development of force, concepts, doctrine, training, organization, and materiel systems.

(2) Consistency ensures that multiple users work from a standard, approved intelligence baseline.

(3) Continuous threat support means that the impact of the threat is considered throughout the life cycle of a materiel system, from its earliest research and development phase through and including postdevelopment product improvements. It assures that organizations and doctrinal developments are supported throughout their conceptual phases and after implementation.

b. A threat support program consists of approved Department of Defense (DOD) and Army intelligence products (documents, data bases, concepts, scenarios) and the procedures designed to respond to threat requirements that are not fulfilled by published intelligence products.

c. Threat support plans will be initiated early in the combat development process to support the conduct of MAA. This ensures that the impact of the threat is considered and applied during the process which may lead to the identification of a requirement for a specific materiel system or a change in organization, doctrine, or training. Threat support plans also will be prepared to support the development of all force, combat, and materiel development programs and studies.

d. At the start of a study or project, the proponent will identify threat support requirements. The senior intelligence officer at each command level is responsible for coordinating and providing threat support to combat and materiel developers and is responsible for the application of the threat in support of programs and studies conducted by his or her command.

e. The relationship between a U.S. system or program and the specific threat is dynamic and reflects changes in tactics, doctrine, and technological advancements. SIOs of proponent commands will maintain a life cycle threat audit trail for each program.

f. The basis or start point for developing the threat to an MAA or specific program, system, or study is the Soviet Battlefield Development Plan (SBDP). If the SBDP is not sufficient for developing a system specific threat, the proponent will use the intelligence products defined in paragraph 2–2 or forward an intelligence production requirement through command channels for tasking to the USAIA, in accord with AR 381–19. The OACSI threat integration staff officer (TISO) will coordinate and assist in the development of threat support requirements, and the application of the threat in support of the development process.

g. Specific guidance for the preparation of threat assessments is contained in paragraph 2–6.

2–2. Intelligence products

Intelligence products are publications and automated data bases that, as a group, address foreign force capabilities in the nearterm (0–5 years), midterm (5–10 years), and far-term (10–20 years). These products constitute Army-approved intelligence for use in developing threat assessments and will be used for satisfying system specific threat support requirements. To ensure consistency throughout the Army intelligence and development communities, HQDA (DAMI–FIT) will publish semiannual listings of approved intelligence products for use in supporting each mission area. Deviations from intelligence contained in these products will only be approved by OACSI. Deviations require conspicuous notation in analysis documentation indicating that a threat excursion was used. The SBDP and other approved intelligence produced by the Army and Defense Intelligence Agency (DIA) will be used for threat development. These baseline products are essential for sustaining the provision of consistent threat throughout the acquisition process, and represent the start point for assessments prior to initiating specific requests for support.

2–3. Threat simulation within Army analyses

Army analyses make extensive use of computerized combat simulations. These simulations are used to evaluate capabilities and determine user and resource requirements in the context of complete force interactions and varying battlefield requirements. To ensure the validity of Army analyses, computerized combat simulations must appropriately represent threat force combat, combat support, and combat service support in a consistent manner. The agency conducting the analysis must know the appropriate models to use as well as their strengths, weaknesses, and limitations. The validity of threat force activity depends on model sensitivity, data input, and decision logic incorporated within the various models employed to conduct the analysis. To achieve threat consistency, commonality, and accuracy within models, the following procedures apply:

a. Intelligence data. The references identified in paragraph 2–2 will be used for threat analysis. Deviations from the intelligence contained within these references may be used for interactive analysis by Army analysis activities; however, such deviations will be documented in the analysis and identified in the assumption portion of all analyses. Study directors will be informed of such deviations and their potential impact.

b. Combat simulation use. Studies and analyses conducted by HQDA and MACOMs often require the use of combat simulations. MACOMs and supporting intelligence officers will establish procedures ensuring that threat data used in the simulations are accurate and current, and portray threat activities and events correctly. TCGs and existing data bases will be used to satisfy the requirement for current and accurate data inputs. Validation of threat portrayed in models under Army Model Improvement Program (AMIP) (AR 5–11) hierarchy of models is the responsibility of OACSI (DAMI–FIT). Validation of threat portrayed in all other models is the responsibility of each MACOM headquarters. Problem areas and events that cannot be portrayed accurately will be fully documented and furnished to OACSI (DAMI–FIT) for approval through the chain of command. Deviations from OACSI–approved scenarios and threat data will also be forwarded to OACSI (DAMI–FIT) for approval through the chain of command. These problems will be identified at each milestone meeting or IPR meeting for consideration by study members. Documentation will include, as a minimum, assumptions, decision rules, uses, limitations, data required, and data currently stored.

c. Combat simulation development. Combat simulations being developed will be fully documented. MACOMs, contract monitors, and intelligence offices supporting these efforts will establish procedures for reviewing threat data and decision rules for accuracy, currency, and correct portrayal of threat activities and events. Existing data bases and intelligence resources will be used to satisfy the requirement. This regulation and AR 381–19 outline procedures for tasking intelligence resources. Validation of threat portrayal in existing models under the AMIP hierarchy of models is the responsibility of OACSI (DAMI–FIT). Validation of threat portrayed in all other models is the responsibility of each MACOM headquarters. Problem areas and events that cannot be portrayed accurately, or deviate from threat guidance, will be identified and fully documented for approval by OACSI (DAMI–FIT). Those identified areas will become agenda items at milestone meetings and program review meetings in order that participants may better understand the capabilities, limitations, and approved deviations of the combat simulations. Documentation will include, as a minimum, assumptions, decision rules, limitations, data required, and data stored.

d. Scenario development. Army analytic agencies require basic guidelines regarding precursory events, time lines, and threat employment concepts in addition to data on threat force structure and weapon systems characteristics. To promote and achieve accuracy, commonality, and consistency within Army analyses, the following guidelines apply to the development of scenarios for threat forces:

(1) The annual DOD Defense Guidance (DG) provides the Services with a plan for the development of the necessary military capabilities to maintain the Nation's security. It will be used to begin development of scenarios intended to support the force and materiel development processes. The DG contains a planning scenario intended to—

(a) Provide a general illustrative sequence of events upon which to base force development planning for the future 10–year timeframe and to assess risks to programed forces.

(b) Provide a common set of U.S. friendly force assumptions for use by the Services in computing the readiness, sustainability, mobility, and modernization of resources.

(2) OACSI will review the DG assumptions for impact on threat and provide scenario development guidance at the beginning of each year.

(a) TRADOC. TRADOC standard scenarios will be used in studies and analysis to identify the Army force modernization needs encompassing organization, doctrine, training, and materiel. The threat scenarios developed by TRADOC and approved by OACSI through timely IPRs, will serve as the base for Army combat and materiel development studies, unless otherwise directed by HQDA. TRADOC will use OACSI–approved threat data and operational concepts to develop standard scenarios. All TRADOC standard scenarios will be reviewed annually to ensure that they are consistent with Army guidance. Army schools, centers, and activities involved in force and materiel development will use this approved scenario for analyses. If threat excursions are employed, they will be highlighted clearly in study reports.

(b) U.S. Army Concepts Analysis Agency. OACSI guidance to CAA on global force employment scenarios will be based on specific study and model requirements. The scenarios developed will provide a common threat basis for annual planning and programing studies conducted for the HQDA Staff. Data will be provided to CAA by OACSI (DAMI–FIT). OACSI will review results of the analysis as appropriate to ensure that intelligence data on threat doctrine and force employment are logical and consistent.

2–4. Threat integration staff officer (TISO)

a. A TISO is designated by the ACSI to function as the HQDA threat integration coordinator for designated mission areas, programs, and materiel systems. The TISO represents OACSI on all aspects of threat support throughout the life cycle or study process. The TISO system complements the HQDA force integration staff officer (FISO) and Department of the Army system coordinator (DASC) system and is designed to foster close coordination among the intelligence community, MACOMs, and Army Staff agencies to ensure the timely integration of threat into the materiel development and acquisition process. The TISO system supplements existing management procedures but does not relieve Army Staff agencies and MACOMs of established responsibilities.

b. The responsibilities of the TISO are as follows:

(1) Represent the ACSI and serve as primary HQDA Staff point of contact for threat integration.

(2) Coordinate the implementation of Army policy relating to threat support.

(3) Establish and manage TCGs for Army MAAs, major and DAP systems, and selected HQDA studies.

(4) Provide timely HQDA threat guidance to those agencies and commands responsible for combat and materiel development.

(5) Coordinate DA approval for all threat assessments written or oral to support major and DAP systems and selected studies.

(6) Coordinate DIA validation of threat assessments written to support systems requiring DSARC decision review. (See DIA Reg 55-3.)

(7) Direct the threat support process to ensure consistent application of intelligence to major and DAP systems.

(8) Maintain a listing of critical intelligence parameters that impact upon the effectiveness, survivability, or security of the U.S. system. Forward CIPs to DIA for incorporation into national collection plans.

(9) Coordinate appropriate OACSI participation to special task forces and special study groups for MACOM managed studies.

(10) Assist combat and materiel developers and the test and evaluation community in generating and articulating requirements for threat support.

(11) Coordinate with DOD, DIA, and other Service intelligence agencies on all aspects of threat support to Army specific or joint Service programs.

(12) In coordination with DCSOPS and DCSRDA, review threat statements or assessments contained in HQDA requirements, decision, and program documents.

(13) Monitor use of threat data during development and operational test and evaluation phases of the materiel development cycle for major and DAP systems to ensure maximum benefit from knowledge of the threat environment.

(14) Establish liaison and maintain close coordination with Army Staff agencies, MACOMs, testing agencies, and other agencies to assure that threat support is timely, consistent, and continuous throughout the life cycle process.

(15) Monitor and ensure quality control of intelligence production requirements in response to materiel development threat requirements.

(16) Recommend as appropriate the establishment of MACOM chaired TCGs.

(17) Represent HQDA at MACOM level TCGs if requested and appropriate.

(18) Attend formal and informal program reviews in the course of materiel life cycle, and determine impact of threat considerations on the progress of system development.

c. OACSI (DAMI-FIT) is the approving authority for either establishing or ending TISO monitorship of systems. Generally, all programs designated as major or DAP systems will be assigned a TISO. Other nonmajor systems will be assigned TISO monitorship on an "as required" basis with the approval of OACSI (DAMI-FIT).

2-5. Threat coordinating groups (TCGs)

a. A TCG is an integrating body between the Army's combat and materiel development activities and the intelligence community to coordinate the provision of timely, consistent, and approved threat support throughout the life cycle or study process. Through the development and implementation of threat support plans, the TCG coordinates the identification, validation, and fulfillment of threat requirements supporting each system or program.

b. The purpose of the TCG is to ensure that all appropriate organizations are informed of the development/execution of the threat support plan, pertinent threat issues, and means for resolution and that they are mutually supportive of the overall effort. The preparation of threat assessments associated with the project or study remain the responsibility of the developer. The TCG chairman will coordinate the approval of threat assessments that are based upon the intelligence data provided in response to user requirements.

c. There are two types of TCGs, system specific and mission area. System specific TCGs coordinate threat support requirements for specific programs. For each major and Designated Acquisition Program, HQDA (DAMI-FIT) will normally establish and chair a TCG. Other programs of particular DA interest may also require a DA level TCG. MACOMs will establish TCGs for nonmajor programs as required. The mission area TCG will be established to coordinate threat support requirements for the MAA process. MAA TCGs will be established by TRADOC. The MAA TCG will serve as the transition vehicle to system or study specific TCGs, at either HQDA or MACOM level.

d. For new programs, system specific TCGs will be formed as early as possible in the life cycle process, but not later than the submission of the JMSNS for major programs or for DAPs. Major and DAP systems which have already passed their production milestones will be considered for TCG support, although priority will be given to new programs and those nearing milestone decision reviews.

e. Membership of each HQDA-managed TCG will consist of representatives from the HQDA Staff, combat and materiel development commands, OTEA, and the intelligence community. Representatives from DIA and other Services will be invited to participate in a TCG if it is a joint program with Army as lead Service or if the TCG needs that Service expertise.

f. The functions of system specific and mission area TCGs are as follows:

(1) System specific TCGs.

(a) Assist the combat and materiel developers in articulating their threat requirements and facilitating the resolution of these requirements from the intelligence community.

(b) Assist in the development of a comprehensive threat support plan based on stated user needs, regulatory requirements, and intelligence resources.

(c) Develop for the user a comprehensive baseline of intelligence products from appropriate approved intelligence documents.

(d) Coordinate and review the combat and materiel developers' critical intelligence parameters and ensure the development of intelligence production requirements in response to identified CIPs.

(e) Review intelligence data and threat portrayed in the concept formulation process and provide recommendations to the appropriate agencies.

(f) Review wargaming models for correct application of threat.

(g) Coordinate and review threat support for developmental and operational testing to include use of scenarios and simulators (that is, ADATS).

(h) Coordinate and review the STAR and threat portions of program management documents, such as the JMSNS, SCP, DCP, COEA, and TSP.

(2) Mission area TCGs.

(a) Provide threat support for the MAA process.

(b) Integrate the results of threat support for specific systems into the total MAA.

(c) Provide for transition of threat support from the MAA to appropriate HQDA or MACOM TCGs established to support major and DAP systems.

2-6. Threat assessments

a. Documents required for the systems acquisition process are known as program management documents (PMD) and are divided into the following three categories:

(1) Requirements documents.

(2) Decision documents.

(3) Program documents.

b. The proponent responsible for developing a specific requirement, decision, or program document will also write the required threat assessment for that document (table 2-1). The threat assessment will provide a summary of the current and projected threat and targets and missions of the proposed system and will emphasize the interactive effects of the system and threat.

c. When drafting threat assessments, the intelligence office supporting the developer will use Army and DIA-approved intelligence products as given in paragraph 2-2.

d. For assistance in preparing a PMD threat assessment to support a major or DAP system, threat support requirements will be forwarded through command channels to OACSI (DAMI-FIT). The TISO, with the assistance and participation of the appropriate TCG, will assist in identifying relevant existing intelligence documents or by tasking new intelligence production in accord with AR 381-19.

e. The appropriate MACOM headquarters will be responsible for coordinating the preparation of PMD threat assessments to support DAIPR or IPR level systems.

f. Threat assessments will be written at the lowest possible classification consistent with user needs. More highly classified supplements will be developed if necessary for program decision. If a threat assessment must be released to the North Atlantic Treaty Organization (NATO), a specific country, or a group of countries, it will be prepared in coordination with DIA. OACSI will coordinate this effort.

g. Approval authorities for PMD threat assessments are indicated in table 2-1. Threat assessments for major and DAP systems will be forwarded through command channels to HQDA (DAMI-FIT), WASH DC 20310-1086, for review and approval.

h. A draft of the complete program management document will accompany the threat assessment when it is forwarded for review and approval.

i. OACSI will forward threat assessments written for materiel systems requiring DSARC review to DIA for validation. In the case of a threat assessment prepared for an Army lead joint Service program, OACSI will coordinate the assessment with the other Services involved before submitting it to DIA.

j. Threat assessments submitted for DA approval will be footnoted to indicate the sources for data. This is required to expedite the approval process.

k. See appendix B for information on the content of PMD threat assessments.

2-7. System Threat Assessment Report (STAR)

a. General. The STAR summarizes the approved threat provided to combat and materiel developers of a specific system. It provides an assessment of the enemy's capabilities to neutralize or degrade a specific U.S. system or system concept as determined by the interactive analysis. This report is RCS exempt in accord with AR 335-15, paragraph 5-2*e*(2).

b. Timing. The initial STAR will be prepared in time to support a milestone I decision. It will be prepared in concert with the concept formulation process and will be updated before each subsequent milestone decision. Significant changes in the threat between the time a STAR has been approved and the arrival of the next milestone will require that the STAR be revised to reflect the threat actually used in the program.

c. Structure.

(1) The STAR will contain the following four major sections:

(a) A description of the U.S. system or system concept.

(b) Threat environment in which the U.S. system is to operate, including targets when appropriate.

(c) Specific threats that will degrade or neutralize the U.S. system's effectiveness during its operational lifetime.

(d) Reasonably expected reactions to development and deployment of the U.S. system.

(2) The approved intelligence supporting the STAR will be summarized rather than republished in its entirety. This reduces the length of the STAR to about 25-30 pages.

(3) Suggested format guidance for the STAR is at appendix C.

d. Content.

(1) The system specific threat will focus on quantifiable threat capabilities relative to the mission and specific performance parameters of the U.S. system. It will describe plausible hostile developments and not simply present technological or mirror image projections.

(2) Conclusions will be based on approved DOD intelligence products. Other analyses, however, are acceptable for the far term, as long as the rationale is included and they are reasonable projections of accepted data.

(3) Once CIPs have been identified, STAR updates will focus on related threat intelligence.

(4) Appendixes will be developed as necessary to support assessments made in the body of the STAR. An appendix will be developed listing critical intelligence parameters.

e. Approval. OACSI will approve STARs for major and DAP systems. A minimum of 20 days is required for OACSI approval. OACSI will obtain DIA validation of STARs for major programs to DSARC milestone reviews. HQ TRADOC and HQ AMC will approve STARs for DAIPR and IPR level systems and provide information copies of MACOM-approved STARs to HQDA (DAMI-FIT).

f. Classification. STAR classification will be limited to SECRET. Higher level supplements may be added as needed.

g. References.

(1) The STAR will be annotated by paragraph to show the sources for data. This is required to expedite the approval process.

(2) A bibliography will be included in the STAR which will list all data sources used in preparation of the document.

2-8. Operations security (OPSEC)

Request for OPSEC support will be forwarded through command channels in accord with AR 530-1.

2-9. Special Access Programs (SAPs)

Threat support for SAPs will follow the same policies and procedures established for systems and programs that fall within the purview of this regulation. Maximum use of approved threat documentation such as STARs for existing programs will be made with appropriate compartmented appendixes. See AR 380-381 for specific regulatory guidance for SAPs.

Section II
Army Studies

2-10. Study directive

a. Each study directive will include, as a minimum, a threat guidance subparagraph. This subparagraph will give the location, general situation, and intensity of combat applicable to the study.

b. Study directives prepared by HQDA in accord with AR 5-5 which require threat support will be coordinated, in draft, with OACSI (DAMI-FIT) to ensure that appropriate threat support tasking has been included.

2-11. Study advisory group (SAG)

For each study, the study sponsor will form a SAG or appoint a study manager. (Hereafter, an appropriate role for the study manager will be implied when the terms "SAG chairman" or "SAG" are used.) SAGs advise study sponsors and give advice and technical guidance to study agencies.

2-12. SAG membership

All studies requiring threat support will have a threat representative on the SAG. OACSI will provide for SAG membership for HQDA-directed studies or those requiring DA-approved threat support.

2-13. Procedures for HQDA-directed studies

a. When designated by OACSI, the USAIA will provide threat analysis and production support to HQDA-directed studies (except those discussed in *b* and *c* below). The SAG chairman will ensure that threat requirements are identified and submitted in writing to OACSI (DAMI-FIT).

b. The SAG chairman will designate an intelligence representative to provide a copy of the minutes of each SAG meeting to HQDA (DAMI-FIT).

c. When a commercial contractor is designated to accomplish a study requiring threat, the statement of work will be coordinated through command channels with HQDA (DAMI-FIT) to ensure that the threat and disposition of the data base are given proper attention. HQDA (DAMI-FIT) will monitor the contract effort and provide threat guidance as needed.

Table 2-1
System Specific Threat Responsibilities Matrix

Type acquisition	Approval level	Type of review	Threat responsibilities[1]	Threat approval
Major Program	SECDEF	ASARC/DSARC		
JMSNS/O&O/LOA/ROC Threats			CBTDEV	OACSI[2]
SCP/DCP/IPS Threats			MATDEV	OACSI
COEA Threat			CBTDEV	OACSI
STAR			CBTDEV/ MATDEV	OACSI
Designated Acquisition Program	SA	ASARC		
O&O/LOA/ROC Threats			CBTDEV	OACSI
SCP/DCP/IPS Threats			MATDEV	OACSI
COEA Threai			CBTDEV	OACSI
STAR			CBTDEV/ MATDEV	OACSI
DAIPR Program	HQDA (DCSRDA)	IPR		
O&O/LOA/LR Threats			CBTDEV	CBTDEV
SCP/DCP/IPS Threats			MATDEV	MATDEV
COEA Threat			CBTDEV	CBTDEV
STAR			CBTDEV/ MATDEV	CBTDEV/ MATDEV
IPR Program	MATDEV	IPR		
O&O/LOA/LR Threats			CBTDEV	CBTDEV
SCP/DCP Threats			MATDEV	MATDEV
COEA Threat			CBTDEV	CBTDEV
STAR			CBTDEV/ MATDEV	CBTDEV/ MATDEV

Notes:
[1] CBTDEV and MATDEV will coordinate the preparation and review of all threat assessments for all four levels of systems.
[2] OACSI will obtain DIA validation of threat assessments (JMSNS, SCP, DCP, IPS, and STARs) written to support materiel systems requiring DSARC decision review.

Appendix A
References

Section I
Required Publications

AR 5–5
Army Studies and Analysis. (Cited in para 2–10.)

AR 5–11
Army Model Improvement Program. (Cited in para 2–3.)

AR 70–1
Army Systems Acquisition Policy and Procedures. (Cited in paras B–2 and B–3.)

AR 380–381
Special Access Programs. (Cited in para 2–9.)

AR 381–19
Intelligence Support. (Cited in paras 2–1 and 2–3.)

AR 530–1
Operations Security (OPSEC). (Cited in para 2–8.)

DIA Regulation No. 55–3
Threat Support for Major System Acquisitions. (Cited in para 2–4*b*(6).)

Section II
Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

AR 1–1
Planning, Programing, and Budgeting Within the Department of the Army

AR 15–14
Systems Acquisition Review Council Procedures

AR 70–17
System/Program/Project/Product Management

AR 71–3
User Testing

AR 71–9
Materiel Objectives and Requirements

AR 381–20
U.S. Army Counterintelligence and Security Support Activities

AR 1000–2
Basic Policies for Systems Acquisition

DODD 5000.1
Major Systems Acquisitions

DODI 5000.2
Major System Acquisition Procedures

Appendix B Program Management Documents Threat Assessments

B–1. Requirements documents

Requirements documents normally are generated by the combat developer in coordination with the materiel developer. Requirements documents which contain threat assessments include the Justification for Major System New Start (JMSNS), Operational and Organizational Plan (O&O), Letter of Agreement (LOA), required operational capability (ROC), letter requirement (LR), and, in the case of a joint Service program, the Joint Service Operational Requirement (JSOR). AR 71–9 contains detailed information on the content and format of these documents. The following paragraphs contain a brief description of, and provide guidance for, the preparation of threat assessments.

a. JMSNS.

(1) The JMSNS documents a major deficiency in a Service's ability to meet mission requirements. The JMSNS justifies the acquisition of a new major system and supports program initiation.

(2) The JMSNS threat narrative provides an assessment of the key threat elements relating to the mission deficiency. Current and projected threat assessments should be provided. The JMSNS threat assessment will emphasize specific threat-driven mission area deficiencies as identified by the MAA process. The JMSNS is restricted to a maximum of three pages, including annexes. The threat assessment, therefore, will normally be limited to three or four paragraphs.

b. O&O Plan.

(1) The O&O Plan supports program initiation for all nonmajor materiel systems.

(2) The content of a threat assessment written for an O&O Plan will be similar to that for a JMSNS. Its length will be limited to about one or two pages.

c. LOA. The LOA is a jointly prepared document in which the combat and materiel developers outline the basic agreements for further investigation of a potential materiel system. It is written to support a Milestone I decision review.

d. ROC. The ROC is prepared by the combat developer in coordination with the materiel developer. It describes the minimum essential operational, technical, and cost data and other information necessary to initiate full scale engineering development or procurement of a materiel system. It is prepared to support a Milestone II decision.

e. LR. An LR is prepared in place of a ROC for acquisition of low-value or commercial items.

f. JSOR. A JSOR is a statement of need for the same end item of materiel for operational employment by the Army and at least one other U.S. military service. It takes the place of a ROC for all joint Service programs.

g. LOA/ROC/JSOR threat assessment. Threat assessments written for each LOA, ROC, and JSOR will describe the mission, organization, operation, or specific system of the threat that the needed materiel system is required to defeat. It will also describe the enemy's current and projected capability to detect, identify, locate, avoid, suppress, destroy, or otherwise counter the U.S. system. To support the evolutionary development of a U.S. system, the threat statement will include an assessment of the probable reactive threat to the system. Intended targets of the U.S. system will also be identified. The threat assessment should summarize the system's capability as determined by interactive analysis to perform its assigned mission in its operational environment against the expected threat. The basic document of an LOA, ROC, or JSOR is limited to four pages. The threat assessment will be about two or three paragraphs. If the materiel development is threat-driven, there should be a clear connection with the deficiency identified in the MAA process or other appropriate requirements study.

B–2. Decision documents

Decision documents are prepared by the materiel developer in coordination with the combat developer and are submitted to the appropriate decision review authority (ASARC, DSARC). As explained in AR 70–1, there are three types of decision documents: system concept paper, decision coordinating paper, and integrated program summary.

a. SCP. The SCP is a 12-page document, excluding annexes, prepared to support a Milestone I decision which summarizes the program status of a materiel system up to that point and provides the acquisition strategy for subsequent development of the program.

b. DCP. The DCP summarizes program status for Milestone II and III. It may not exceed 18 pages, excluding annexes.

c. IPS. The IPS provides a detailed summary of a program at Milestones II and III. It is only required when the decision authority Defense Acquisition Authority, Army Acquisition Executive (AAE), or DCSRDA desires more information than that contained in the DCP. The IPS is restricted to 30 pages.

d. SCP/DCP/IPS threat assessments. The content of a threat assessment for an SCP, DCP, or IPS will be similar to that prepared for an LOA, ROC, or JSOR, as described in paragraph B–1g and normally will be derived from the STAR. The length of an SCP or DCP threat assessment will be limited to about one or two pages. An IPS threat assessment will be about four or five pages. If the materiel development is threat-driven there should be a clear connection with the deficiency identified in the MAA process or other appropriate requirements study.

B–3. Program documents

Program documents are developed to implement the overall acquisition strategy of a materiel system. As explained in AR 70–1, these documents include individual plans that are reviewed and approved and become part of the program management documents. The cost and operational effectiveness analysis (COEA) report is a program document which contains a summary of threat provided in support of the COEA process.

a. COEA report. This document provides decision-makers with the results of analyses conducted to evaluate the merits of alternatives and to understand the likely effect of each choice. It provides information on the costs and projected operational and training effectiveness of alternative materiel systems and programs. Threat support provided by the COEA process is a major factor in determining the validity of alternatives presented in the COEA report.

b. COEA threat.

(1) The COEA report will contain a section summarizing the threat support provided to the COEA process. The COEA threat will describe the full range of threats to the proposed materiel system. Excursions may be presented as long as the rationale is included and they are reasonable projections of accepted data. There is no standard length for a COEA threat; however, references may be made to existing DA– or DIA–approved threat products to avoid duplication of data.

(2) Threat support will cover the entire projected life cycle of the U.S. system, beginning at initial operational capability (IOC). It will provide quantifiable near-term, midterm and far-term S&TI and operational art, employment, and deployment data.

Appendix C
STAR Format Guidance

C–1. Preliminary pages

a. Title page. This page shows the title, preparing agency, information cutoff date, U.S. systems project office, and, for major programs only, the MACOM/DA/DIA validation statement and date.

b. Table of contents and illustrations.

c. Executive summary. This will include a concise description of the future operational threat environment, the system specific threat, the reactive threat that could affect program decisions, and, if appropriate, a target assessment. The timeframe should start at IOC of the U.S. system and continue through its expected operational lifetime. The executive summary should be a complete, autonomous threat overview. It should be specific and sharply focused to provide the key intelligence judgments applicable to the CIP and the particular milestone issues. If the materiel development is threat-driven there should be a clear connection with the deficiency identified in the MAA process or other appropriate requirements study.

C–2. Body

a. The body of the STAR will focus on the quantifiable threat capabilities relative to the mission and specific performance parameters of the U.S. system. The body will consist of the following:

(1) *Introduction.* Give a brief opening statement, which may include a short synopsis of the mission need for the U.S. system.

(2) *U.S. system description.* Provide a concise description of the system. For the sake of brevity, this may be done by referring to existing program documents which already describe the system. In either case, contents will include the mission, available physical and technical characteristics (to include such electronic parameters as frequency bands, radiated power, modulation), method of operation, IOC, and life span data (detailed parameters may only become available as the program develops). If development of the U.S. system would cause a marked change in the threat to related elements (launch platform, associated command, control, communications, and so forth), then these elements should be addressed in the system description. The system description, alternative system concepts, subsystems, potential protective measures, and system operational concepts under consideration will be provided and validated by the developer.

(3) *Operational threat environment.* Give a generalized overview of the operational, physical, and technological environment in which the system will function during its lifetime, and, if applicable, the targets it is designed to engage. Developments and trends which can be expected to affect mission capability during the U.S. system's lifetime should be projected out to the end of the life cycle. Areas covered should include enemy operational concepts, organizations, equipment and tactics affecting system mission(s), and operations. Threat content and emphasis will vary from program to program. The requirement to describe the operational threat environment may be satisfied by references to the relevant portions of existing threat intelligence documents, such as the SBDP and other approved products.

(4) *Targets.* Include an analysis, if applicable, of the actual capabilities of projected enemy targets the U.S. system is designated to engage. Target employment, characteristics, command and control, and numbers should be included. Types and density of targets might also be covered along with such common parameters as the thickness and types of armor to be defeated. If detailed technical specifications for individual target models are required, reference may be made to appropriate approved intelligence products.

(5) *System specific threat (SST).* Provide an assessment of the threat to the mission capabilities of the U.S. system throughout its operational lifetime. Timeframes for threat snapshots are at IOC of the U.S. system and at IOC plus 10 years. Threat assessments should integrate doctrine, force level, and means (conventional, electronic, nuclear, chemical, advanced weapons, or others, as appropriate). Detail and certainty will decrease as projections extend into the far-term. Confidence in key judgments should be expressed in estimative terms to the maximum extent possible. Analysis will be responsive to CIPs. Reference may be made to existing DA- or DIA-approved intelligence products that provide any of the information concerning the SST to a U.S. system. The SST will include the following:

(a) Threat at IOC of U.S. system.

1. Descriptions of opposing weapons systems.

2. Magnitude of the threat (projected force levels).

3. An integrated assessment of the threat to the U.S. system (hostile employment doctrine, force levels, and equipment) is considered together.

(b) Follow-on system specific threat. A snapshot of the threat at IOC plus 10 years. This should also assess developments which would serve to degrade the U.S. system's capability to the end of its life cycle. Appropriate items to be included are as follows:

1. System description.

2. Magnitude of threat.

3. Threat integration.

(6) *Reactive threat.* Describe to the maximum extent possible changes which might reasonably be expected to occur in hostile doctrine, strategy, tactics, force levels, and weapon systems as a result of the development and deployment of the U.S. system. Assessment of each reactive threat should consider, as a minimum, projections of—

(a) Modifications in doctrine, strategy, and tactics.

(b) New systems or modifications to present systems. Also give the description and likely deployment.

(c) Changes in force levels.

(d) Threat integration. This should consist of an integrated assessment of the potential reactive threat to the U.S. system.

C–3. Appendixes

Specific appendixes will be developed as appropriate to support the threat analysis contained in the body of the STAR or to provide additional detail. As a minimum, an appendix listing critical intelligence parameters identified by the program manager will be developed.

C–4. Bibliography

An annotated bibliography will be developed listing all source documents, models, or scenarios (to include U.S. system data) used to develop the information contained in the STAR.

Glossary

Section I Abbreviations

AAE
Army Acquisition Executive

ADATS
Army Development and Acquisition of Threat Simulators

AFPDA
Army force planning data and assumption

AMC
U.S. Army Materiel Command

ASARC
Army Systems Acquisition Review Council

CBTDEV
combat developer

CIP
critical intelligence parameter

COEA
cost and operational effectiveness analysis

DA
Department of the Army

DAIPR
Department of the Army in-process review

DAP
Designated Acquisition Program

DASC
Department of Army system coordinator

DCP
decision coordinating paper

DCSRDA
Deputy Chief of Staff for Research, Development, and Acquisition

DG
Defense Guidance

DIA
Defense Intelligence Agency

DSARC
Defense Systems Acquisition Review Council

DT
development testing

FDTE
force development testing and experimentation

FISO
force integration staff officer

HQDA
Headquarters, Department of the Army

IOC
initial operational capability

IPR
in-process review

IPS
integrated program summary

JMSNS
Justification for Major System New Start

JSOR
Joint Service Operational Requirement

LOA
Letter of Agreement

LR
letter requirement

LRRDAP
Long-range Research, Development, and Acquisition Plan

MAA
mission area analysis

MACOM
major Army command

MATDEV
materiel developer

NATO
North Atlantic Treaty Organization

NDI
nondevelopment item

OACSI
Office of the Assistant Chief of Staff for Intelligence

ODCSOPS
Office of the Deputy Chief of Staff for Operations and Plans

ODCSRDA
Office of the Deputy Chief of Staff for Research, Development, and Acquisition

O&O
operational and organizational

OPSEC
operations security

OT
operational test

OTE
operational test and evaluation

OTEA
Operational Test and Evaluation Agency

PIP
Product Improvement Proposals

PM
program, project, or product manager

PMD
program management documents

RDA
research, development, and acquisition

ROC
required operational capability

SAG
study advisory group

SAP
Special Access Program

SCORES
Scenario Oriented Recurring Evaluation System

SCP
system concept paper

SECDEF
Secretary of Defense

SSG
special study group

SST
system specific threat

S&TI
scientific and technical intelligence

STAR
System Threat Assessment Report

STF
special task force

TISO
threat integration staff officer

TCG
threat coordinating group

TRADOC
U.S. Army Training and Doctrine Command

TSP
threat support program

USAIA
U.S. Army Intelligence Agency

Section II Terms

Combat developer
Command or agency that formulates doctrine, concepts, organization, materiel requirements, and objectives. This represents the user community in the materiel acquisition process.

Coordinate
The process of seeking concurrence from one or more organizations or agencies on the adequacy of a specific draft assessment, estimate, or report. It is intended to increase a product's factual accuracy, clarify its judgments, and resolve disagreements on threat issues.

Cost and operational effectiveness analysis
Comparison between costs to develop, produce, distribute, and maintain a materiel system, and the ability of the system to meet the requirement for eliminating or reducing a force or mission deficiency.

Critical intelligence parameters
Those threat characteristics (such as numbers, types, mix, or characteristics of actual or projected threat systems) identified by service program managers that would critically impact on the effectiveness, survivability, security, or cost of a U.S. system.

DA in-process review program
Materiel system designated by the DCSOPS in coordination with the DCSRDA based on importance, complexity, and resource requirements. Program review is accomplished by an in-process review conducted by the materiel developer. IPR minutes from key milestones require HQDA (DCSRDA) approval.

Decision coordinating paper
A top-level summary document prepared by AMC that identifies alternatives, goals, thresholds, and threshold ranges to support Milestone II and Milestone III decisions.

Designated Acquisition Program
Materiel system designated by the Army Acquisition Executive (AAE) based on importance, complexity, and resource requirements. DAPs are reviewed by the Army Systems Acquisition Review Council and require AAE approval of key milestones.

In-process review
Review of a project or program at critical points to evaluate status and make recommendations to the decision authority. Conducted by the materiel developer.

In-Process Review Program
All programs not designated otherwise are IPR programs. Program review is accomplished by an in-process review conducted by the materiel developer. No higher review is necessary if IPR participants agree on the proposed acquisition strategy.

Integrated program summary
A top-level document prepared by AMC which summarizes in greater detail than the DCP various facets of the implementation plan of the Service for a major system acquisition. It will be prepared to support a Milestone II or III decision only if the Defense Acquisition Executive or Army Acquisition Executive determines that the DCP lacks sufficient information on which to base a decision.

Intelligence
The product resulting from the collection, evaluation, analysis, integration, and interpretation of all information concerning one of more aspects of foreign countries or areas, which is immediately or potentially significant to the development of plans, policies, and operations.

Intelligence production requirement
A stated need for the production of intelligence on a general or specific subject, program, system, or weapon.

Interactive analysis
A study, such as a COEA, performed by, or under the auspices of, Service program management elements to examine the interaction between a proposed U.S. system and the threat it is intended to encounter during its operational lifetime.

Joint Service Operational Requirement
A statement of need for the same end item for use by the Army and at least one other military service. Army proposed JSORs usually are directed by higher authority and are prepared and processed following ROC procedures and format as much as possible.

Justification for Major System New Start
Identifies and supports the need for new or improved mission capability when costs exceed $200 million RDTE or $1 billion in procurement (FY 80 dollars). Support program initiation.

Letter of Agreement
A jointly prepared and authenticated document in which the combat developer and materiel developer outline the basic agreements for further investigation of a potential materiel system. An LOA is written to support a Milestone I decision.

Letter requirement
An abbreviated procedure, prepared in place of the ROC, for acquisition of low-value or commercial items of which the cost will not exceed $6 million RDTE and $12 million procurement for 1 year, or $50 million RDTE and procurement for 5 years (FY80 dollars).

Major program
Materiel system designated by the Secretary of Defense (SECDEF) based on risk, urgency of need, congressional interest, joint Service involvement and resource requirements. The system acquisition process is reviewed by the Defense Systems Acquisition Review Council and requires SECDEF approval for major milestones.

Materiel developer
Command or agency responsible for research, development, and production of a system in response to approved requirements.

Materiel system
An item, system, or all systems of materiel. This includes all required system support elements.

Mission area analysis
Assessment of capability of a force to perform within a particular mission area. Designed to discover deficiencies in doctrine, organizations, training, and materiel and to identify means of correcting these deficiencies. MAA provides a basis for applying advanced technology to future Army operations.

Operational and organizational plan
Contains an operational, organizational, training, and logistical plan for use to assess current forces and to evaluate proposals for changes to Army forces and doctrine. Approval by the combat developer constitutes program initiation for all programs except those requiring a JMSNS.

Production
Conversion of information or intelligence information into finished intelligence through integration, analysis, evaluation, and/or interpretation of all available data and the preparation of intelligence products in support of known or anticipated user requirements.

Reactive threat
Changes which might reasonably be expected to occur in hostile doctrine, strategy, tactics, force levels, and weapon systems as a result of the development and deployment of the U.S. system.

Required operational capability
An HQDA document which states the minimal essential operational, technical, logistical, and cost information necessary to initiate full-scale development or acquisition of a materiel system. A ROC is written to support a Milestone II decision.

Scenario oriented recurring evaluation system
An evaluation technique and framework used to develop TRADOC scenarios to identify performance shortfalls and to address organizations, doctrine, tactics, training, and materiel.

System concept paper
The decision management document prepared by AMC that summarizes the results of concept exploration up to Milestone I, describes the acquisition strategy, and establishes goals and thresholds to be reviewed at the next milestone.

System Threat Assessment Report
The STAR is a threat assessment tailored to and focused on a particular U.S. system. It contains an integrated assessment of projected enemy capabilities (doctrine, tactics, hardware, organization, and forces) to limit, neutralize, or destroy a specific U.S. system. The STAR will serve as the basic threat

document supporting system development. It is a dynamic document that will be continually updated and refined as the program develops. The STAR is written to support all three decision milestones. It will be approved/validated in support of the ASARC/DSARC.

Threat

a. The ability of an enemy or potential enemy to limit, neutralize, or destroy the effectiveness of a current or projected mission, organization, or item of equipment. The statement of that threat is prepared in sufficient detail to support Army planning and development of concepts, doctrine, training, and materiel.

b. A statement of a capability prepared in necessary detail, in the context of its relationship to a specific program or project, to provide support for Army planning and development of operational concepts, doctrine, and materiel.

Threat approval

The evaluation of, and concurrence with, either a threat intelligence document or threat assessment. Threat approval is synonymous with threat validation.

Threat assessment

An evaluation of an enemy's or potential enemy's current or projected capability to limit, neutralize, or destroy the effectiveness of a mission, organization, or item of equipment. It involves the application of threat analysis to a specific mission, organization, or item of equipment within the context of a military operation. Threat assessments considers the project of threat analysis vis-a-vis a U.S. force and includes the perceived military judgments of the evaluated threat force.

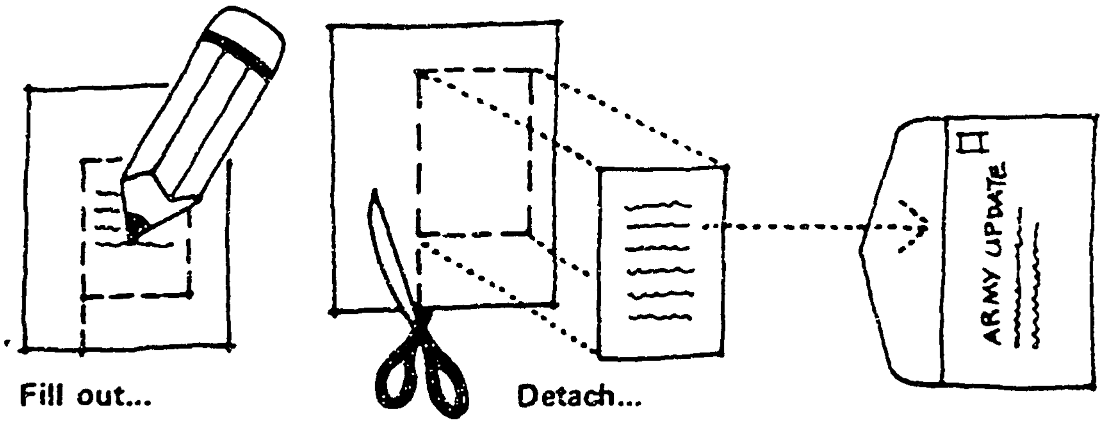
Threat coordinating group

A group formed to manage threat support to the force and materiel development process throughout the entire life cycle of the systems process.

Threat validation

The evaluation of and concurrence with either a threat intelligence document or a threat assessment. Threat validation is synonymous with threat approval.

U.S. GOVERNMENT PRINTING OFFICE: 19[illegible]



Place in envelope and mail to...

Army UPDATE Publications
800 West Church Road
Mechanicsburg, PA 17055-3198

Instructions for completing the subscription card in this volume.

PART 1: This section is for internal use within your unit.

PART 2:
Publication Account Number
(Insert 5-digit account number. The first block will be a letter and each succeeding block will be a number.) If you do not have an established account and wish to open one, complete DA Form 12.

Quantity Required
(Insert total number of copies your unit requires.)

Name/Address of Unit
(Insert full name, address, and zip code as it appears on the labels that you receive on mailings from the Baltimore AG Publications Center.)

Subscription Information: Valid account holders must submit the enclosed subscription card if they want to either increase or decrease their present quantity.

Resupply: Limited copies of this UPDATE publication are available from the Baltimore Publications Center. Complete DA Form 4569, USAAGPC Requisition Code Sheet accordingly.

Army UPDATE Publications Subscription Card

AR 381-11

PART 1. FOR COMPLETION BY USER OF PUBLICATION
Record copy requirements for your section. Pass card to unit publication clerk for consolidation of total subscription requirement.

Name of section. ____________

Number of copies desired for section use. ____________

PART 2. FOR COMPLETION BY UNIT PUBLICATION CLERK
Use one of these cards to consolidate all section requirements into one unit subscription, then mail immediately.

Abstract from DA Form 12-99

PUBLICATION ACCOUNT NO. □ □ □ □ □		
FORM NUMBER	BLOCK NUMBER	QUANTITY REQUIRED
12-14	0966	

Publications Clerk... These blocks <u>MUST</u> be filled in.

Unit Name and Address

DA FORM 12-13, FEBRUARY 1985